

IN THE U.S. PATENT AND TRADEMARK OFFICE

#2  
JC986 U.S. PTO  
09/991932  
11/26/01

Applicant(s): MIYAGAWA, Akiko et al.

Application No.:

Group:

Filed: November 26, 2001

Examiner:

For: ILLEGAL ACCESS DATA HANDLING APPARATUS AND METHOD FOR  
HANDLING ILLEGAL ACCESS DATA

L E T T E R

Assistant Commissioner for Patents  
Box Patent Application  
Washington, D.C. 20231

November 26, 2001  
2565-0238P

Sir:

Under the provisions of 35 USC 119 and 37 CFR 1.55(a), the applicant hereby claims the right of priority based on the following application(s):

| <u>Country</u> | <u>Application No.</u> | <u>Filed</u> |
|----------------|------------------------|--------------|
| JAPAN          | 2001-036436            | 02/14/01     |

A certified copy of the above-noted application(s) is(are) attached hereto.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to deposit Account No. 02-2448 for any additional fees required under 37 C.F.R. 1.16 or under 37 C.F.R. 1.17; particularly, extension of time fees.

Respectfully submitted,

BIRCH, STEWART, KOLASCH & BIRCH, LLP

By:

MICHAEL K. MUTTER  
Reg. No. 29,680  
P. O. Box 747  
Falls Church, Virginia 22040-0747

Attachment  
(703) 205-8000  
/sll

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2001年 2月14日

出 願 番 号

Application Number:

特願2001-036436

出 願 人  
Applicant(s):

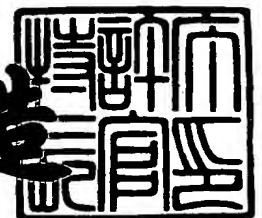
三菱電機株式会社



2001年 6月 4日

特 許 庁 長 官  
Commissioner,  
Japan Patent Office

及 川 耕 造



出証番号 出証特2001-3051882

【書類名】 特許願

【整理番号】 529273JP01

【提出日】 平成13年 2月14日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社  
社内

【氏名】 宮川 明子

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社  
社内

【氏名】 稲田 徹

【発明者】

【住所又は居所】 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社  
社内

【氏名】 後沢 忍

【特許出願人】

【識別番号】 000006013

【氏名又は名称】 三菱電機株式会社

【代理人】

【識別番号】 100099461

【弁理士】

【氏名又は名称】 溝井 章司

【選任した代理人】

【識別番号】 100111497

【弁理士】

【氏名又は名称】 波田 啓子

【選任した代理人】

【識別番号】 100111800

【弁理士】

【氏名又は名称】 竹内 三明

【手数料の表示】

【予納台帳番号】 056177

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9903016

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 不正侵入データ対策処理装置及び不正侵入データ対策処理方法

【特許請求の範囲】

【請求項 1】 所定の内部通信ネットワーク外に配置され、

前記内部通信ネットワークに不正に侵入する目的で前記内部通信ネットワーク外に配置されたいずれかのデータ通信装置より送信された不正侵入データを受信し、受信した前記不正侵入データに対する対策処理を行うことを特徴とする不正侵入データ対策処理装置。

【請求項 2】 前記不正侵入データ対策処理装置は、

前記内部通信ネットワーク内に配置されたデータ通信装置と前記内部通信ネットワーク外に配置されたデータ通信装置との間のデータ通信の中継を行うとともに前記不正侵入データを検知する不正侵入データ検知装置に接続され、

前記不正侵入データ検知装置より前記不正侵入データを受信することを特徴とする請求項 1 に記載の不正侵入データ対策処理装置。

【請求項 3】 前記不正侵入データ対策処理装置は、

前記不正侵入データ検知装置より、前記不正侵入データを受信するデータ受信部と、

前記データ受信部により受信された前記不正侵入データを解析するデータ解析部と、

前記データ解析部による解析結果に基づき、前記不正侵入データに対する応答データを生成する応答データ生成部と、

前記応答データ生成部により生成された前記応答データを前記不正侵入データ検知装置に対して送信するデータ送信部とを有することを特徴とする請求項 2 に記載の不正侵入データ対策処理装置。

【請求項 4】 前記データ受信部は、

前記不正侵入データ検知装置より、前記不正侵入データ検知装置によりカプセル処理された不正侵入データを受信し、

前記不正侵入データ対策処理装置は、更に、

前記データ受信部により受信されたカプセル処理された不正侵入データのカプ

セル処理を解除して不正侵入データを抽出するとともに、前記応答データに対してカプセル処理を行うカプセル処理部を有し、

前記データ送信部は、

前記カプセル処理部によりカプセル処理された応答データを前記不正侵入データ検知装置に対して送信することを特徴とする請求項 3 に記載の不正侵入データ対策処理装置。

【請求項 5】 前記応答データ生成部は、

前記内部通信ネットワーク内に配置された特定のデータ通信装置が前記不正侵入データを受信した場合に、前記特定のデータ通信装置が前記不正侵入データに対して生成する応答データと同じ内容の応答データを生成することを特徴とする請求項 3 に記載の不正侵入データ対策処理装置。

【請求項 6】 前記データ受信部は、

前記不正侵入データ検知装置より、前記不正侵入データ検知装置の通信履歴を示す通信履歴情報を受信し、

前記データ解析部は、

前記データ受信部により受信された前記通信履歴情報を解析し、前記通信履歴情報の解析結果に基づき前記内部通信ネットワーク外に配置された所定のデータ通信装置から送信されるデータを不正侵入データに指定する不正侵入データ指定情報を生成し、

前記データ送信部は、

前記データ解析部により生成された前記不正侵入データ指定情報を前記不正侵入データ検知装置に送信することを特徴とする請求項 3 に記載の不正侵入データ対策処理装置。

【請求項 7】 前記データ受信部は、

前記不正侵入データ検知装置より、データ認証に用いる認証情報が添付された不正侵入データを受信し、

前記カプセル処理部は、前記認証情報を用いて前記不正侵入データのデータ認証を行うことを特徴とする請求項 4 に記載の不正侵入データ対策処理装置。

【請求項 8】 前記カプセル処理部は、

前記応答データのデータ認証に用いる認証情報を前記応答データに添付し、  
前記データ送信部は、

前記カプセル処理部により認証情報が添付された応答データを前記不正侵入データ検知装置に送信することを特徴とする請求項 7 に記載の不正侵入データ対策処理装置。

【請求項 9】 所定の内部通信ネットワーク外において、

前記内部通信ネットワークに不正に侵入する目的で前記内部通信ネットワーク外に配置されたいずれかのデータ通信装置より送信された不正侵入データを受信し、受信した前記不正侵入データに対する対策処理を行うことを特徴とする不正侵入データ対策処理方法。

【請求項 10】 前記不正侵入データ対策処理方法は、

前記内部通信ネットワーク内に配置されたデータ通信装置と前記内部通信ネットワーク外に配置されたデータ通信装置との間のデータ通信の中継を行うとともに前記不正侵入データを検知する不正侵入データ検知装置と通信を行い、

前記不正侵入データ検知装置より前記不正侵入データを受信することを特徴とする請求項 9 に記載の不正侵入データ対策処理方法。

【請求項 11】 前記不正侵入データ対策処理方法は、

前記不正侵入データ検知装置より、前記不正侵入データを受信するデータ受信ステップと、

前記データ受信ステップにより受信された前記不正侵入データを解析するデータ解析ステップと、

前記データ解析ステップによる解析結果に基づき、前記不正侵入データに対する応答データを生成する応答データ生成ステップと、

前記応答データ生成ステップにより生成された前記応答データを前記不正侵入データ検知装置に対して送信するデータ送信ステップとを有することを特徴とする請求項 10 に記載の不正侵入データ対策処理方法。

【請求項 12】 前記応答データ生成ステップは、

前記内部通信ネットワーク内に配置された特定のデータ通信装置が前記不正侵入データを受信した場合に、前記特定のデータ通信装置が前記不正侵入データに

対して生成する応答データと同じ内容の応答データを生成することを特徴とする請求項10に記載の不正侵入データ対策処理方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

この発明は、コンピュータネットワークのセキュリティサポート契約者に対し、不正侵入を検知した契約者のネットワーク機器からの情報により、不正侵入者をおとりサーバに誘導する手段を提供する管理システムに関するものである。

【0002】

【従来の技術】

従来のネットワークシステムでは、不正侵入検知機能を備えたネットワーク構成機器や管理装置によって、企業などの組織単位で独自にセキュリティ対策を施すのが主流であった。

例えば、特開2000-90031によれば、ルータ間にネットワーク不正解析システムを設け、通信に不正を検出すると、通信当事者間の通信を傍受する方式、特開2000-47987では、不正アクセスを検知した場合、正規データベースとは別に用意した擬似データベースへの誘導を行い、正規データの流出を防ぐ方式、特開平6-6347では、セキュリティ管理装置を設け、不正アクセスを検知したネットワーク構成機器が管理装置に不正アクセス報告を通知し、管理装置にてセキュリティを集中管理する方式がある。

これらは、すべて企業などネットワークを運営する顧客がシステムを導入し、顧客自ら管理する方式である。

【0003】

【発明が解決しようとする課題】

しかしながら、従来のネットワークシステムでは、組織の規模が小さい場合、ネットワーク管理者の確保や管理ノウハウの教育が難しいという問題があった。

また、専任のネットワーク管理者の確保が可能な場合でも、ネットワーク管理者の責任のもと、すべてネットワーク機器や管理システムを管理していたため、ネットワーク機器の設定、変更、保守に多大な労力が必要であった。



また、ネットワーク構成の変更や新しい不正侵入の手法に対応するための新規導入およびバージョンアップのコストも大きく、迅速に対応できていなかった。

例えば、特開2000-47987や特開平6-6347では、不正アクセス検出後の対処方法は管理者の采配に委ねられており、特開2000-47987では、擬似データベースへ侵入者を誘導する対策が取られているものの、ネットワークを運営している組織で擬似データベースの設置を行わなければならない。

【0004】

この発明は、上記のような問題点を解決するためになされたもので、ネットワーク利用者もしくは管理者に代わって、不正侵入の防御や対処を行う集中管理システムを提供することを目的とする。

【0005】

このような集中管理システムを利用するサービス利用者側は、おとりサーバ（擬似サーバ）の設置やログ解析、応答パケットの作成といった対処を専門のサービス業者に委託することによって、ネットワーク管理のコストを軽減することができるという利点がある。

また、サービス提供者側は、サービス利用者のネットワーク機器の状況を遠隔地から常時把握することができるため、サービス利用者のところに、出向かずとも迅速な対応が可能となる。

【0006】

【課題を解決するための手段】

本発明に係る不正侵入データ対策処理装置は、  
所定の内部通信ネットワーク外に配置され、  
前記内部通信ネットワークに不正に侵入する目的で前記内部通信ネットワーク外に配置されたいずれかのデータ通信装置より送信された不正侵入データを受信し、受信した前記不正侵入データに対する対策処理を行うことを特徴とする。

【0007】

前記不正侵入データ対策処理装置は、  
前記内部通信ネットワーク内に配置されたデータ通信装置と前記内部通信ネットワーク外に配置されたデータ通信装置との間のデータ通信の中継を行うとと

もに前記不正侵入データを検知する不正侵入データ検知装置に接続され、

前記不正侵入データ検知装置より前記不正侵入データを受信することを特徴とする。

【0008】

前記不正侵入データ対策処理装置は、

前記不正侵入データ検知装置より、前記不正侵入データを受信するデータ受信部と、

前記データ受信部により受信された前記不正侵入データを解析するデータ解析部と、

前記データ解析部による解析結果に基づき、前記不正侵入データに対する応答データを生成する応答データ生成部と、

前記応答データ生成部により生成された前記応答データを前記不正侵入データ検知装置に対して送信するデータ送信部とを有することを特徴とする。

【0009】

前記データ受信部は、

前記不正侵入データ検知装置より、前記不正侵入データ検知装置によりカプセル処理された不正侵入データを受信し、

前記不正侵入データ対策処理装置は、更に、

前記データ受信部により受信されたカプセル処理された不正侵入データのカプセル処理を解除して不正侵入データを抽出するとともに、前記応答データに対してカプセル処理を行うカプセル処理部を有し、

前記データ送信部は、

前記カプセル処理部によりカプセル処理された応答データを前記不正侵入データ検知装置に対して送信することを特徴とする。

【0010】

前記応答データ生成部は、

前記内部通信ネットワーク内に配置された特定のデータ通信装置が前記不正侵入データを受信した場合に、前記特定のデータ通信装置が前記不正侵入データに対して生成する応答データと同じ内容の応答データを生成することを特徴とする。

【0011】

前記データ受信部は、

前記不正侵入データ検知装置より、前記不正侵入データ検知装置の通信履歴を示す通信履歴情報を受信し、

前記データ解析部は、

前記データ受信部により受信された前記通信履歴情報を解析し、前記通信履歴情報の解析結果に基づき前記内部通信ネットワーク外に配置された所定のデータ通信装置から送信されるデータを不正侵入データに指定する不正侵入データ指定情報を生成し、

前記データ送信部は、

前記データ解析部により生成された前記不正侵入データ指定情報を前記不正侵入データ検知装置に送信することを特徴とする。

【0012】

前記データ受信部は、

前記不正侵入データ検知装置より、データ認証に用いる認証情報が添付された不正侵入データを受信し、

前記カプセル処理部は、前記認証情報を用いて前記不正侵入データのデータ認証を行うことを特徴とする。

【0013】

前記カプセル処理部は、

前記応答データのデータ認証に用いる認証情報を前記応答データに添付し、

前記データ送信部は、

前記カプセル処理部により認証情報が添付された応答データを前記不正侵入データ検知装置に送信することを特徴とする。

【0014】

本発明に係る不正侵入データ対策処理方法は、

所定の内部通信ネットワーク外において、

前記内部通信ネットワークに不正に侵入する目的で前記内部通信ネットワーク

外に配置されたいずれかのデータ通信装置より送信された不正侵入データを受信し、受信した前記不正侵入データに対する対策処理を行うことを特徴とする。

【0015】

前記不正侵入データ対策処理方法は、

前記内部通信ネットワーク内に配置されたデータ通信装置と前記内部通信ネットワーク外に配置されたデータ通信装置との間のデータ通信の中継を行うとともに前記不正侵入データを検知する不正侵入データ検知装置と通信を行い、

前記不正侵入データ検知装置より前記不正侵入データを受信することを特徴とする。

【0016】

前記不正侵入データ対策処理方法は、

前記不正侵入データ検知装置より、前記不正侵入データを受信するデータ受信ステップと、

前記データ受信ステップにより受信された前記不正侵入データを解析するデータ解析ステップと、

前記データ解析ステップによる解析結果に基づき、前記不正侵入データに対する応答データを生成する応答データ生成ステップと、

前記応答データ生成ステップにより生成された前記応答データを前記不正侵入データ検知装置に対して送信するデータ送信ステップとを有することを特徴とする。

【0017】

前記応答データ生成ステップは、

前記内部通信ネットワーク内に配置された特定のデータ通信装置が前記不正侵入データを受信した場合に、前記特定のデータ通信装置が前記不正侵入データに対して生成する応答データと同じ内容の応答データを生成することを特徴とする。

【発明の実施の形態】

実施の形態 1.

図1は、この発明に係る不正侵入データ対策処理装置を含むネットワークシス

テムの全体構成図である。

図1において、1は不正侵入対策サービスを実施する管理代行業者のデータセンタであり、11はデータセンタ内に設置された管理システム、12は、顧客情報を格納する顧客データベース、13は、不正侵入者を誘導し、情報を取得するためのおとりサーバ、14は、不正侵入情報を解析する際に用いられる知識ベースである。

2はインターネット、3は不正侵入対策サービスのサービス契約者が使用しているネットワーク機器、4はサービス契約者が使用する一般端末、5はサービス契約者が保持している不正侵入者の攻撃対象となる攻撃対象サーバ、6は不正侵入者の端末である。

ここで、管理システム11及びおとりサーバ13は、不正侵入データ対策処理装置として機能し、ネットワーク機器3は、不正侵入データ検知装置として機能する。

また、ネットワーク機器3、一般端末4、攻撃対象サーバ5は、同一の内部通信ネットワークに属する。

#### 【0018】

また、図2は、ネットワーク機器3の機能ブロック図を示している。

ネットワーク機器3は、データの受信および送信を行うデータ収集/送出部31と、一般的な通信か管理システム11からのおとりサーバへの誘導パケット（応答パケット）かを判別する識別情報判別部32と、不正侵入パケットを検出する不正侵入検出部33と、不正侵入パケットもしくはログデータを管理システム11に転送するためにエンカプセル処理を施したり、管理システム11から送られた応答パケットのデカプセル処理を行うパケットカプセル処理部34と、ネットワーク機器3を通過したデータを記録するログ取得部35から構成されている。

#### 【0019】

また、図3は、管理システムの機能ブロック図を示している。

管理システム11は、データの受信および送信を行うデータ受信/送信部111、受信したパケットが契約者からのものかを照会する顧客照会部112、ネッ

トワーク機器3から入手したデータの種別を判別するデータ種別判別部113、ネットワーク機器3から転送された、エンカプセルされた侵入パケットもしくはログデータのデカプセル処理とネットワーク機器3へ送信する応答パケット（応答データ）のエンカプセル処理を行うパケットカプセル処理部114、入手したログデータおよび侵入パケットを解析する不正データ解析部115から構成される。

また、データセンタ1には、この他、管理システム11と情報をやりとりする顧客データベース12、おとりサーバ13、知識ベース14がある。

なお、おとりサーバ13は、不正侵入パケットに対する応答データ（応答パケット）を生成する応答データ生成部として機能する。

#### 【0020】

図4にネットワーク機器3、管理システム11が送受信する通信パケットの構成について示す。

パケットP1は、不正侵入パケットである。パケットP1は、不正侵入者端末6から送信され、ネットワーク機器3により受信される。

パケットP2は、パケットP1をエンカプセル化したパケットで、識別情報を含む不正侵入パケットの情報を転送する。パケットP2は、ネットワーク機器3から管理システム11へ送信される。

パケットP3は、エンカプセル化された応答パケットで、識別情報を含む不正侵入者に対する応答パケット情報を転送する。パケットP3は、管理システム11からネットワーク機器3へ送信される。

パケットP4は、パケットP3をデカプセル化したパケットで、攻撃対象サーバ5からの応答を模擬したおとりサーバ13からの応答パケットである。パケットP4には、攻撃対象サーバ5が応答する内容と同じ情報が格納されており、本来そのままではインターネット上には送出できないが、パケットP3に示すようにエンカプセル化することによってネットワーク機器3への転送を可能にしている。

#### 【0021】

次にネットワークシステム全体の動きについて説明する。

図5は、不正侵入者が内部通信ネットワークに不正侵入した場合の対策処理の流れを示す。

まず、ある不正侵入者端末6がある契約者のネットワーク（内部通信ネットワーク）内に設置されたサーバ（攻撃対象サーバ）5に不正侵入しようとして、不正侵入パケットP1を送信したとする（ステップ101）。

これに対して、ネットワーク機器3において、不正侵入パケットP1を検出する。不正侵入パケットP1を検出したネットワーク機器3は、不正侵入パケットP1（侵入パケット情報）をエンカプセル化してパケットP2を生成し、パケットP2をデータセンタ1に転送する（ステップ102）。これによりネットワーク機器3は、不正侵入パケットP1による攻撃対象サーバ5への不正侵入を防ぐことができる。

次に、データセンタ1の管理システム11では、ネットワーク機器3からパケットP2を受信し、受信したパケットP2を解析し、攻撃対象サーバ5からの応答に見せかけた、おとりサーバ13からの応答パケットP4をエンカプセル化してパケットP3を生成し、パケットP3をネットワーク機器3に送り返す（ステップ103）。

次に、ネットワーク機器3は、管理システム11よりパケットP3を受信し、受信したパケットP3をデカプセル化して応答パケットP4を取りだし、不正侵入者端末6に対して応答パケットP4を送信する（ステップ104）。不正侵入者は、応答パケットP4を攻撃対象サーバ5からの応答だと思い込み、おとりサーバ13に侵入を開始する。

不正侵入者端末6とおとりサーバ13との交信は、毎回ステップ101～ステップ104の手順により行なわれる。おとりサーバ13でのログ解析により不正侵入のより詳細な手口が明らかになる。

#### 【0022】

次にネットワーク機器3の動作について説明する。

図6に、ネットワーク機器3における通信パケットの処理についてフローチャートを示す。

まず、ネットワーク機器3はデータ収集/送出部31より、通信パケットを受

信すると（ステップ 3 0 1）、識別情報判別部 3 2 で、そのパケットが管理システム 1 1 からのエンカプセル化された応答パケット P 3 なのか、単なる中継パケットなのかを受信パケットの識別情報により判別する（ステップ 3 0 2）。

この結果、エンカプセル化された応答パケット P 3 である場合、パケットカプセル処理部 3 4 で、エンカプセル化された応答パケット P 3 のデカプセル処理を行い（ステップ 3 0 3）、不正侵入者端末 6 への応答パケット P 4 として不正侵入者端末 6 に送信する（ステップ 3 0 6）。

一方、単なる中継パケットである場合、不正侵入検出部 3 3 で、不正侵入パケット P 1 かどうかのチェックを行う（ステップ 3 0 4）。ここで、不正侵入パケット P 1 であると判断された場合は、不正侵入パケット P 1 を管理システム 1 1 に転送するため、パケットカプセル処理部 3 4 で不正侵入パケット P 1 をエンカプセルしてパケット P 2 とし（ステップ 3 0 5）、エンカプセル化した不正侵入パケット P 2 をデータ収集／送出部 3 1 から管理システム 1 1 に送信する（ステップ 3 0 6）。

ステップ 3 0 4 の不正侵入チェックにより、正常パケットと判断された場合は、そのままデータ収集／送出部 3 1 から送信先にパケットを中継する（ステップ 3 0 6）。

#### 【 0 0 2 3 】

次に管理システム 1 1 の動作について説明する。

図 7 に、管理システム 1 1 における契約者のネットワーク機器 3 からの受信パケットに対する処理の流れを示す。

まず、管理システム 1 1 は、データ受信／送信部 1 1 1 より、通信パケットを受信すると顧客照会部 1 1 2 で顧客データベース 1 2 を参照し、契約者からのパケットであるかどうかを照合する。この照合に成功しなかったパケットは、不正データとして廃棄するか、管理システムの別タスクで処理する（本発明の範囲外）。

受信パケットの照合に成功した場合、データ種別判別部 1 1 3 により、ネットワーク機器 3 から送信されたパケットのデータが不正侵入パケットを転送したものの（パケット P 2）であるか否かを判別する。



次に、受信したパケットP2は、ネットワーク機器3によってエンカプセルされているため、このパケットP2をパケットカプセル処理部114で、デカプセル処理する。

#### 【0024】

次に、パケットカプセル処理部114でデカプセル処理された不正侵入パケットP1は、不正データ解析部115に渡され、不正データ解析部115は、知識ベース14を参照しながら、抽出された不正侵入パケットP1の解析を行う。知識ベース14には、この解析結果が反映され、今後の解析のための参考事例として追加される。不正データ解析部115は、解析結果をおとりサーバ13に通知し、おとりサーバ13から応答パケットP4を受け取る。応答パケットP4は、不正侵入パケットP1が、攻撃対象サーバ5に受信されたとした場合に、不正侵入パケットに対する攻撃対象サーバ5からの応答と同様の情報を有するパケットである。

この応答パケットP4を攻撃対象サーバ5からネットワーク機器3経由で送信されたパケットに見せかけるため、パケットカプセル処理部114でエンカプセルしてパケットP3とした後、データ受信/送信部111からネットワーク機器3に対してパケットP3を送信する。

この後、ネットワーク機器3では、前述したように、パケットP3をデカプセル処理して、応答パケットP4を抽出し、抽出した応答パケットP4を不正侵入者端末6へ送信する。

#### 【0025】

以上のように、ネットワーク機器3で検出した不正侵入パケットをネットワーク機器3自身で対処するのではなく、管理システム11に転送することによって応答パケットを獲得し、不正侵入者を代行業者のデータセンタ内に設置されたおとりサーバに誘導するようにしているので、顧客のネットワークとは独立した侵入対処サービスを実現することができる。

#### 【0026】

実施の形態2.

以上の実施の形態1では、不正侵入者端末からの不正侵入パケットをネットワ

ーク機器3からデータセンタ1へ転送するようにしたものであるが、次に、不正侵入パケットの早期発見のためネットワーク機器3のログ情報をデータセンタ1へ転送する実施の形態を示す。

図8は、このような場合のネットワークシステム全体の動きを示したものである。

#### 【0027】

図において、ステップ101～ステップ104は、実施の形態1において説明したものと同様であり、本実施の形態においては、ステップ105及びステップ106について説明する。

ネットワーク機器3は、ログ取得部35（図2）により、常に外部からアクセス情報を記録している。このログ情報（通信履歴情報）をエンカプセル化し、管理システム11からの命令もしくはネットワーク機器3自身の定期的なトリガにより管理システム11にパケットP5として転送する（ステップ105）。

ここで、パケットP5の構成を図9に示す。パケットP5は、ログ情報をエンカプセル化したパケットで、ネットワーク機器のログ情報を管理システムに転送するパケットである。。

次に、管理システム11では、パケットカプセル処理部114がパケットP5をデカプセル化し、不正データ解析部115がログ情報を解析する。ここで、問題のあった場合、即ち、不正侵入パケットの疑いのあるパケットが発見された場合は、ネットワーク機器3における不正侵入検出部33の設定情報を更新するため、管理システム11は新しい侵入検出設定情報をネットワーク機器3に送信する（ステップ106）。ここで、侵入検出設定情報とは、ネットワーク機器3に対して不正侵入パケットの疑いがあるパケットを通知し、不正侵入パケットの疑いのあるパケットを送信した端末より以後送信されたパケットを不正侵入パケットとして取り扱うようにネットワーク機器3に対して指示する情報である。即ち、侵入検出設定情報は、不正侵入データ指定情報に相当する。また、侵入検出設定情報は、不正データ解析部115により生成される。

以降、不正侵入の疑いのある送信元からのアクセスは、ネットワーク機器3の不正侵入検出部33にて不正侵入パケットと判断される。例えば、端末6からの

アクセスログを管理システム11が不正と判断した場合、端末6からのアクセスを拒否する設定情報をネットワーク機器3に送信する。この結果、ネットワーク機器3は、端末6からのアクセス（ステップ101）を不正侵入パケットとして検出し、端末6からのパケット（P1：不正侵入パケット）をエンカプセル化した後（P2）、管理システム11に転送する（ステップ102）。以降の処理手段は、実施の形態1と同様である。

#### 【0028】

本形態に関するネットワーク機器3および管理システム11の振舞いは、実施の形態1にほぼ等しい。

ただし、管理システム11において、図6に示すデータ種別判別部113は、受信データに含まれる識別情報から、ネットワーク機器3からの受信パケットがエンカプセル化された不正侵入パケットP2ではなく、ログ情報パケットP5であることを判別する。そして、不正データ解析部115において、ログ情報パケットP5の解析を行う。

また、管理システム11では、不正データ解析部115は、不正侵入パケットの疑いがあるパケットを発見した場合、新しい侵入設定検出情報を生成し、データ受信／送信部111は、生成された新しい侵入設定検出情報をネットワーク機器3に送信する。

#### 【0029】

以上のように、ネットワーク機器3のログ情報を管理システム11に転送することによって集中的な解析を依頼し、その結果、応答パケットを獲得し、不正侵入者を代行業者のデータセンタ内に設置されたおとりサーバに誘導するようにしているので、顧客のネットワークとは独立した侵入対処サービスを実現することができる他、直接の攻撃ではなくとも不正侵入のおそれのあるパケットの侵入を防止することにより、不正侵入の早期発見につながる。

#### 【0030】

実施の形態3.

以上の実施の形態1および2では、転送するパケットをエンカプセル化し、識別情報により、転送するデータ内容を判別している。

次に、本実施の形態において、管理システム 1 1 およびネットワーク機器 3 にて送受信するパケットに認証情報を付加する場合について示す。

【 0 0 3 1 】

図 1 0 において、パケット P 2 を例に認証情報を付加したパケット P 2 H を示す。

パケット P 2 H では、識別情報以降のデータを入力値とするハッシュ等の認証情報を識別情報の前に付加している。

ネットワーク機器 3 における認証情報の付加および認証情報チェックは、パケットカプセル処理部 3 4 のエンカプセル／デカプセル処理で行う。管理システム 1 1 における認証情報の付加および認証情報チェックは、パケットカプセル処理部 1 1 4 のエンカプセル／デカプセル処理で行う。

なお、上記の例では、パケット P 2 に認証情報が付加されたパケット P 2 H を説明したが、同様な構成によりパケット P 3 に認証情報が付加されたパケット P 3 H の送受信も行うことができる。

【 0 0 3 2 】

以上のように、通信パケットに認証情報を追加することによって、管理システムとネットワーク機器との間の通信のセキュリティを向上させる効果がある。

【 0 0 3 3 】

なお、以上の実施の形態 1 ～実施の形態 3 では、本発明に係る不正侵入データ対策処理装置について説明してきたが、同様の処理手順により本発明に係る不正侵入データ対策処理方法を実現することもできる。

【 0 0 3 4 】

ここで、以上にて説明してきた本発明の特徴を示すと以下のようなになる。

本発明は、コンピュータネットワークシステムにおける不正侵入対策に関して、サポート契約者のネットワークセキュリティ集中管理サービスを提供する。

集中管理サービスの一つとして、不正侵入者をサポート提供者のおとりサーバに誘導する。

サービス利用者のネットワーク機器は、不正侵入を検出すると、不正侵入パケットをサービス提供者のデータセンタ内の管理システムに制御情報を施し（エン

カプセル処理)、転送する。データセンタには、管理システム、擬似サーバ(ここではおとりサーバと呼ぶ)等が設置されている。おとりサーバは、不正侵入者の標的となっていたサービス利用者の攻撃対象サーバに見せかけて誘導するためのもので、攻撃対象サーバと同じ応答を返す。管理システムでは、転送された不正侵入パケットの制御情報を解いて(デカプセル処理)解析する。また、おとりサーバからの応答をエンカプセルし、ネットワーク機器に転送する。

管理システムからの応答パケットを受信したネットワーク機器は、応答パケットをデカプセルし、送出する。不正侵入者はこの応答パケットを攻撃対象サーバとの応答だと思い込むが、ネットワーク機器を介して、データセンタのおとりサーバとやりとりしていることとなり、おとりサーバに誘導される。

#### 【0035】

本発明は、コンピュータネットワークシステムにおける不正侵入対策に関して、サポート契約者のネットワークセキュリティ集中管理サービスを提供する。

集中管理サービスの一つとして、不正侵入者をサポート提供者のおとりサーバに誘導する。

サービス利用者のネットワーク機器は、定期的にログ情報をエンカプセル化して、サービス提供者に転送する。データセンタの管理システムでは、ログ情報を解析し、不正が認められた場合、管理システムからの通知によりネットワーク機器の不正侵入検出の設定情報を更新することを特徴とする。

#### 【0036】

本発明は、集中管理サービスが送受信するパケットに関して、認証情報の負荷または暗号化により、セキュリティ強度を向上させることを特徴とする。

#### 【0037】

##### 【発明の効果】

本発明によれば、ネットワーク機器で検出した不正侵入パケットをネットワーク機器自身で対処するのではなく、管理システムに転送することによって応答パケットを獲得し、不正侵入者を代行業者のデータセンタ内に設置されたおとりサーバに誘導するようにしているので、顧客のネットワークとは独立した侵入対処サービスを実現することができる。

【0038】

また、本発明によれば、直接の攻撃ではなくとも不正侵入のおそれのあるパケットの侵入を防止することにより、不正侵入に対する有効な対策を行うことができる。

【0039】

また、本発明によれば、通信パケットに認証情報を追加することによって、管理システムとネットワーク機器との間の通信のセキュリティを向上させる効果がある。

【図面の簡単な説明】

【図1】 ネットワークシステムの全体構成を示す図。

【図2】 ネットワーク機器の機能ブロックを示す図。

【図3】 データセンタの機能ブロックを示す図。

【図4】 通信パケットP1～P4の構成を示す図。

【図5】 実施の形態1における不正侵入パケット対策処理の手順を示す図

【図6】 ネットワーク機器の処理フローを示す図。

【図7】 データセンタの処理フローを示す図。

【図8】 実施の形態2における不正侵入パケット対策処理の手順を示す図

【図9】 通信パケットP5の構成を示す図。

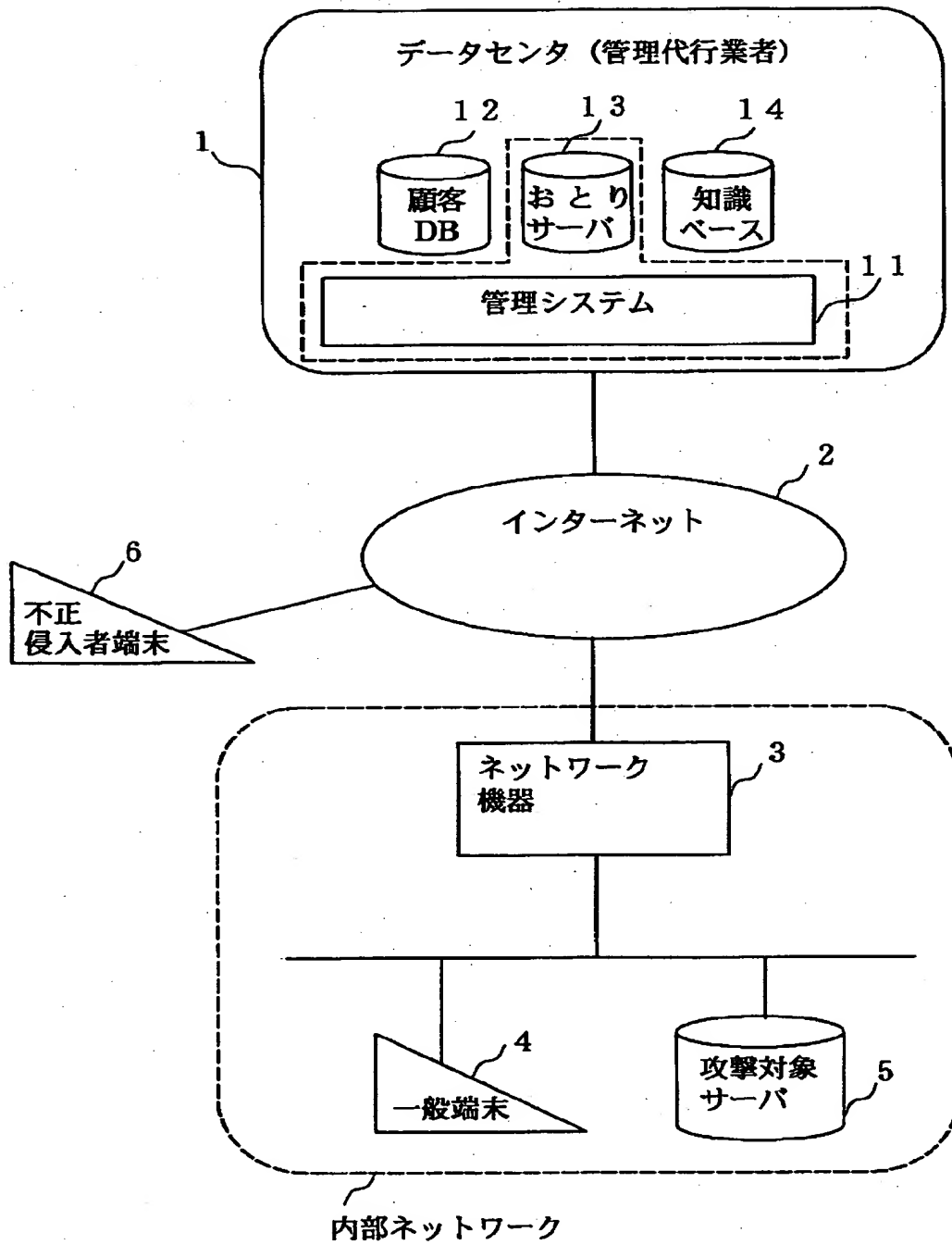
【図10】 通信パケットP2Hの構成を示す図。

【符号の説明】

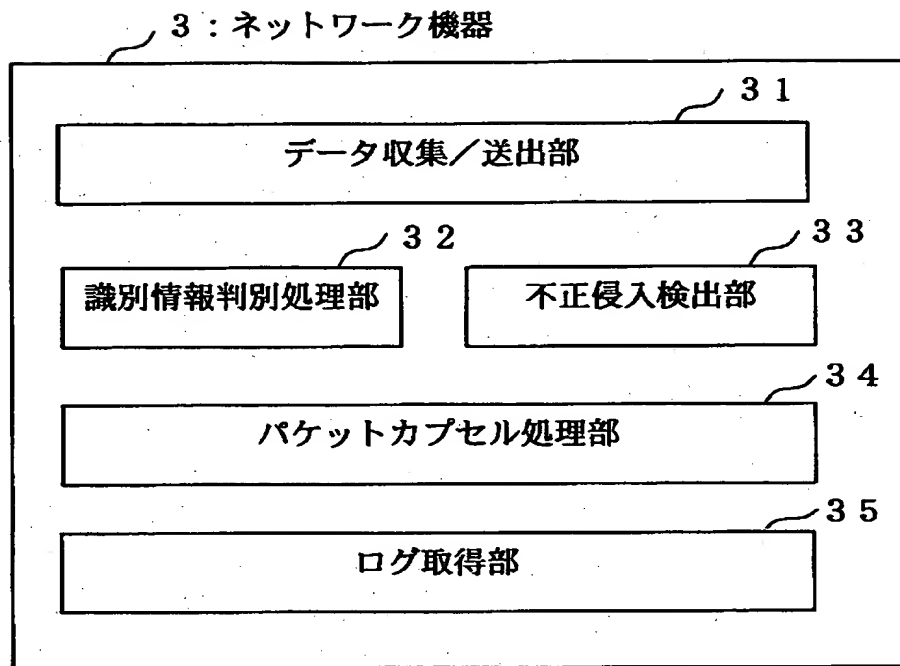
1 データセンタ、2 インターネット、3 ネットワーク機器、4 一般端末、5 攻撃対象サーバ、6 不正侵入者端末、11 管理システム、12 顧客データベース、13 おとりサーバ、14 知識ベース。

【書類名】 図面

【図 1】

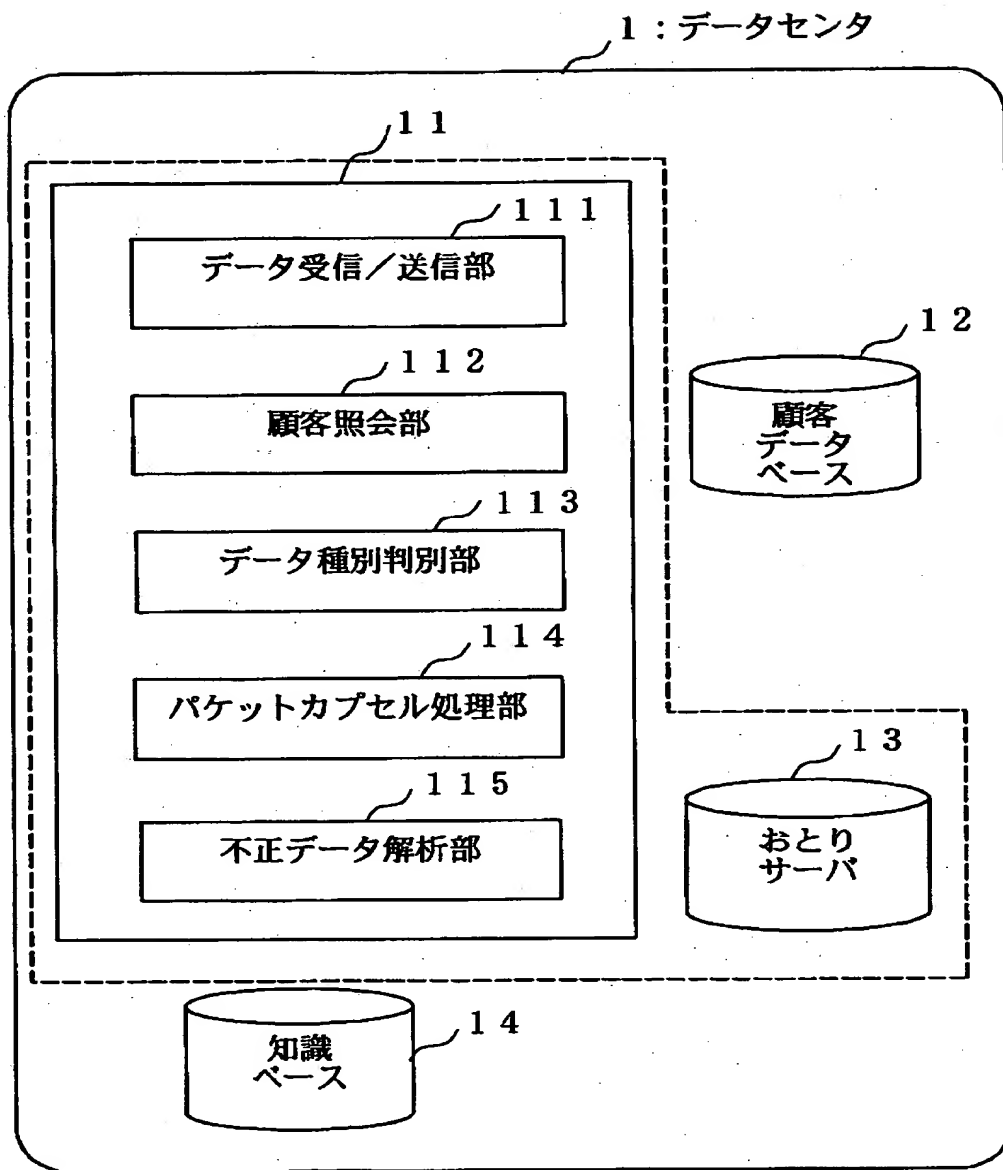


【図 2】

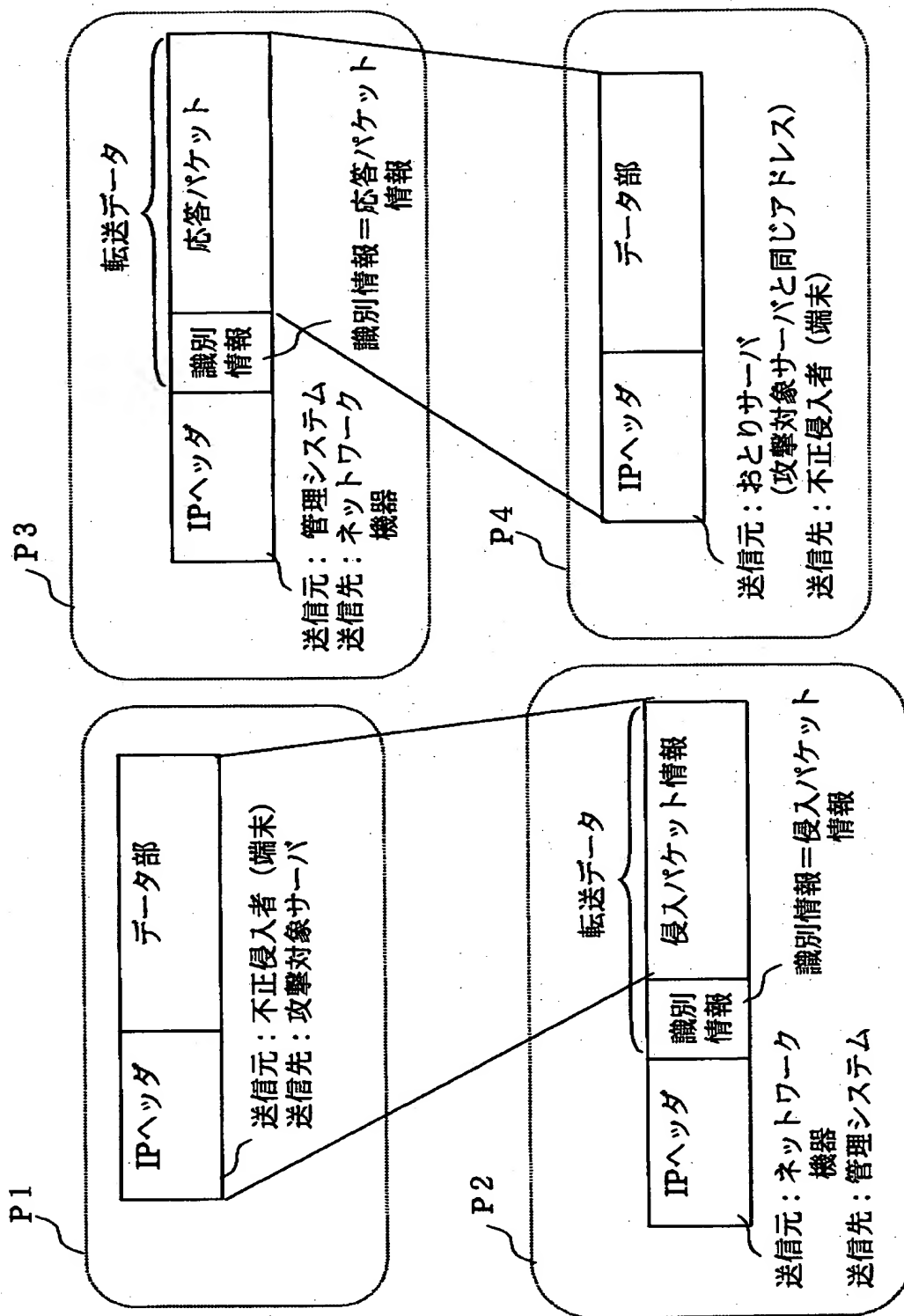




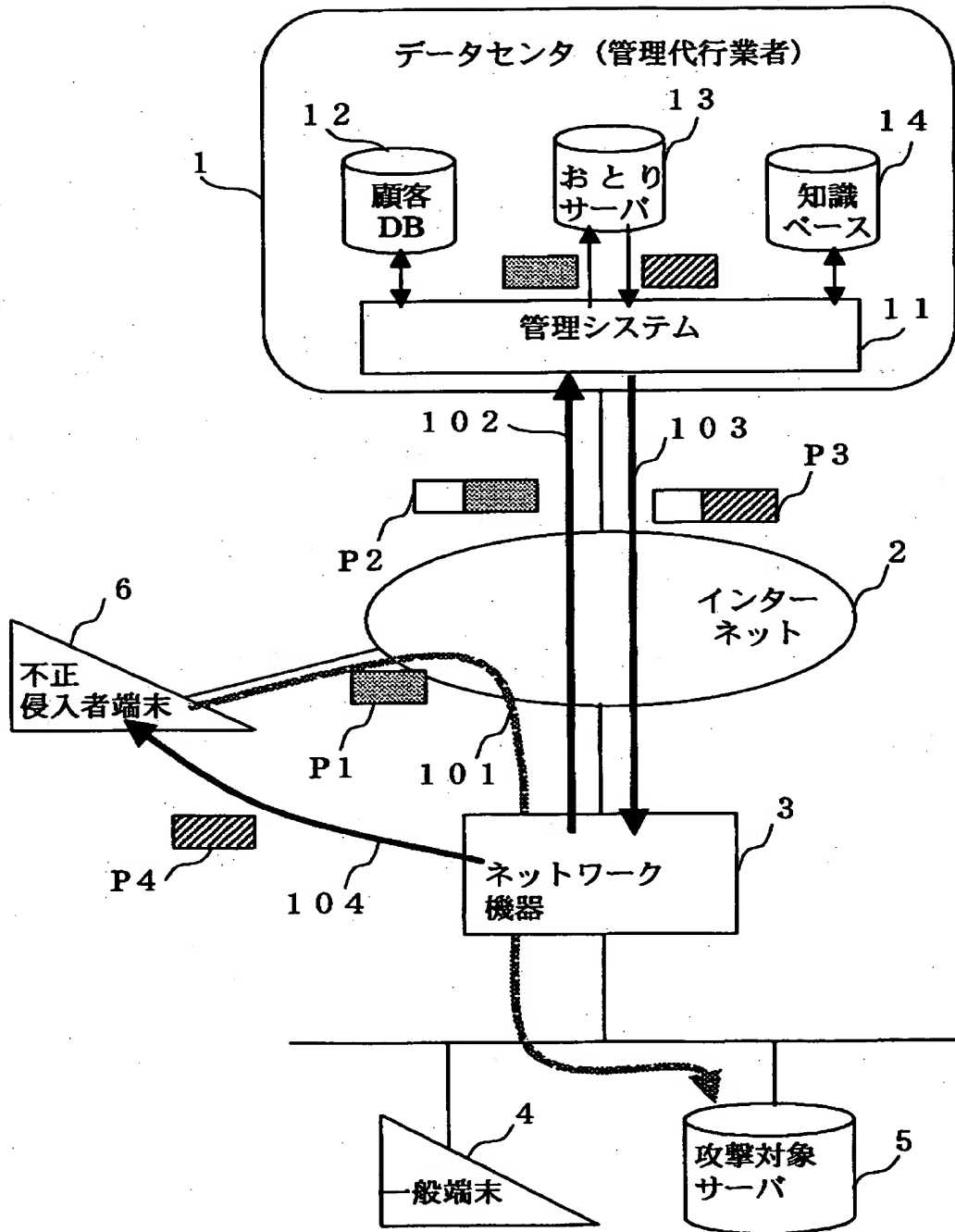
【図3】



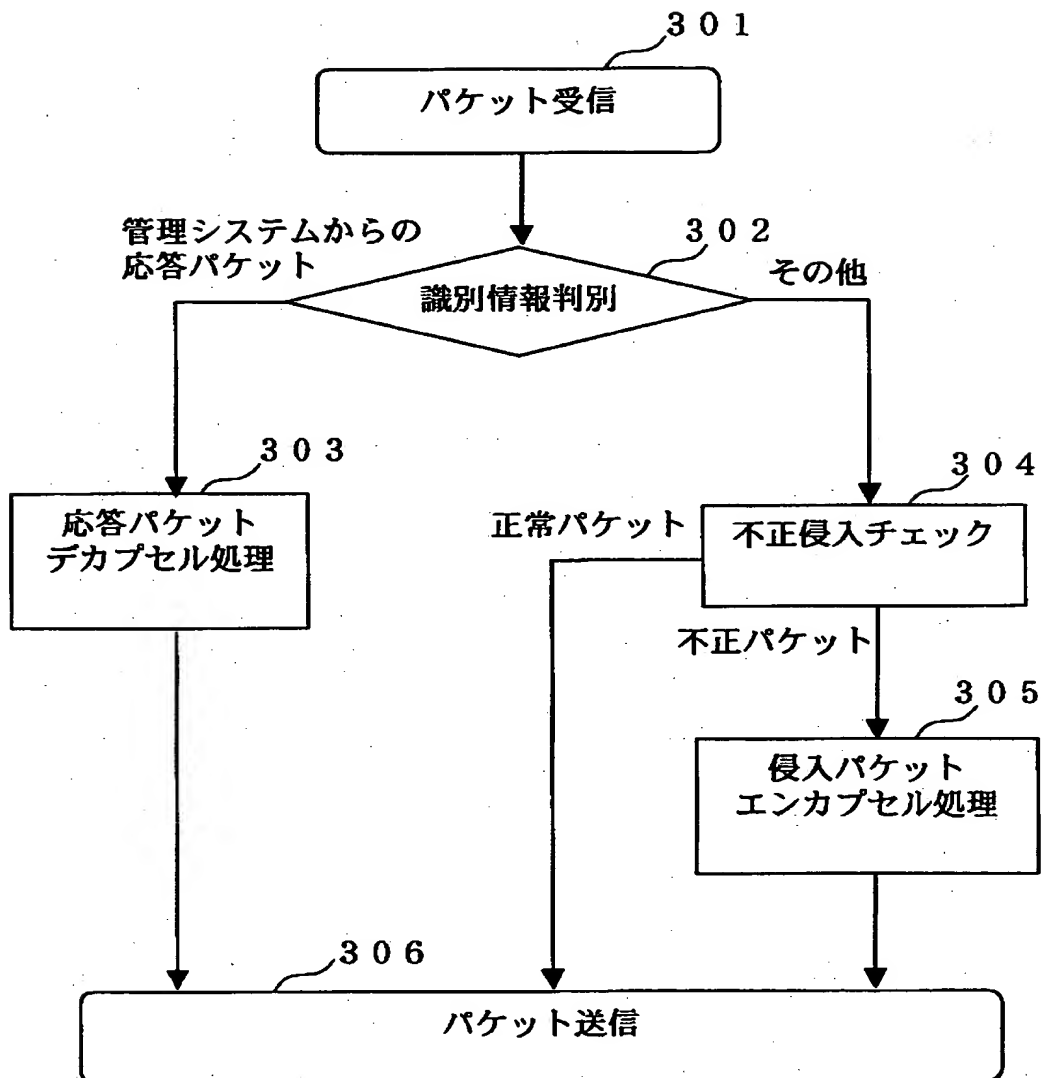
【図4】



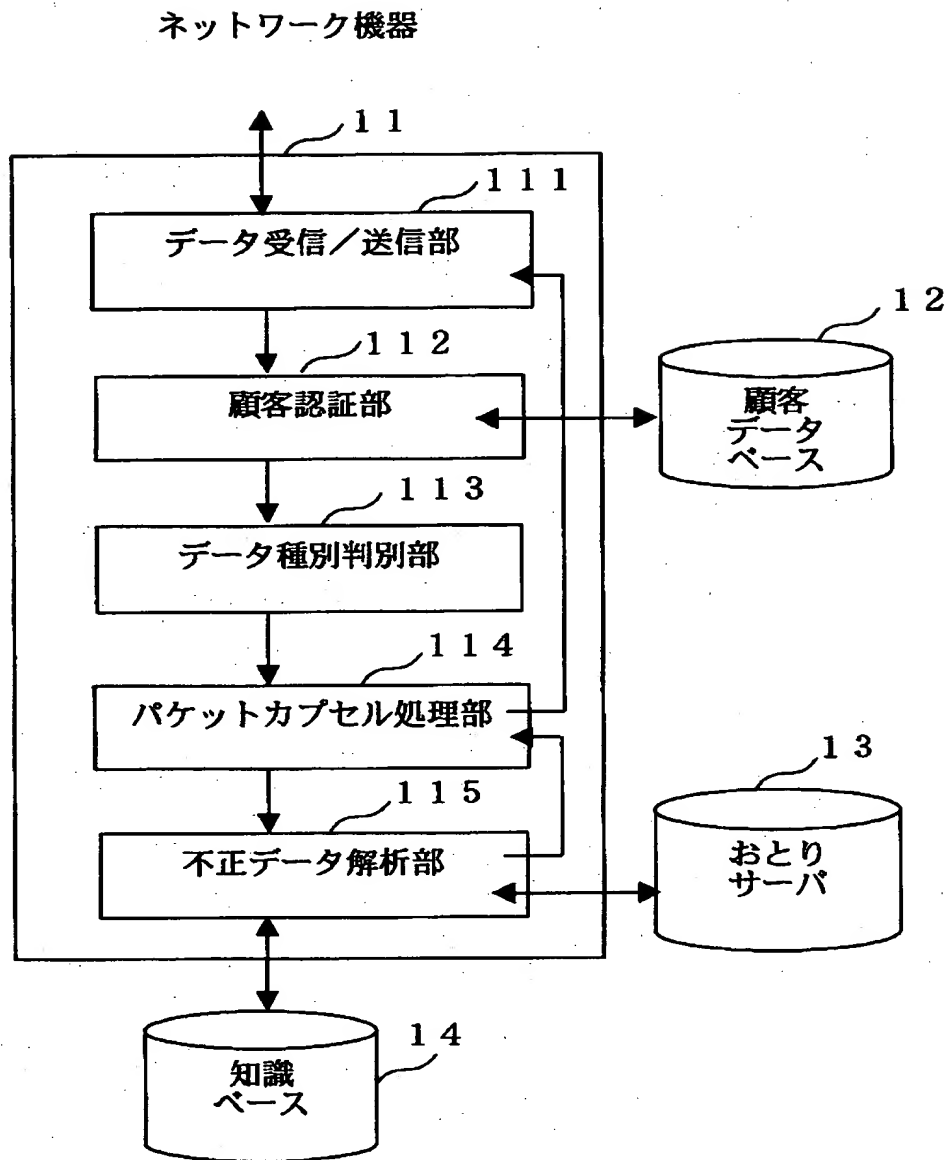
【図 5】



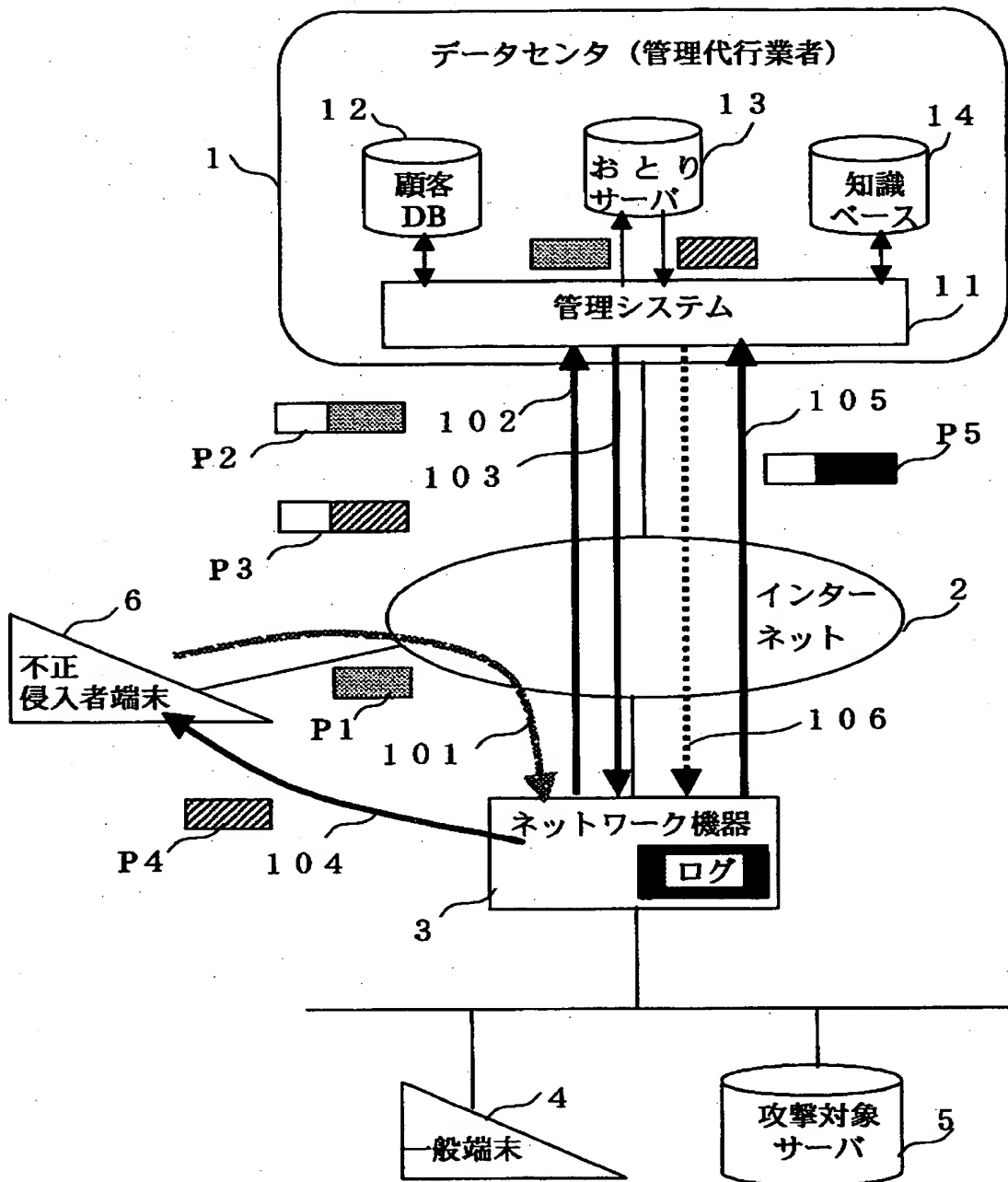
【図 6】



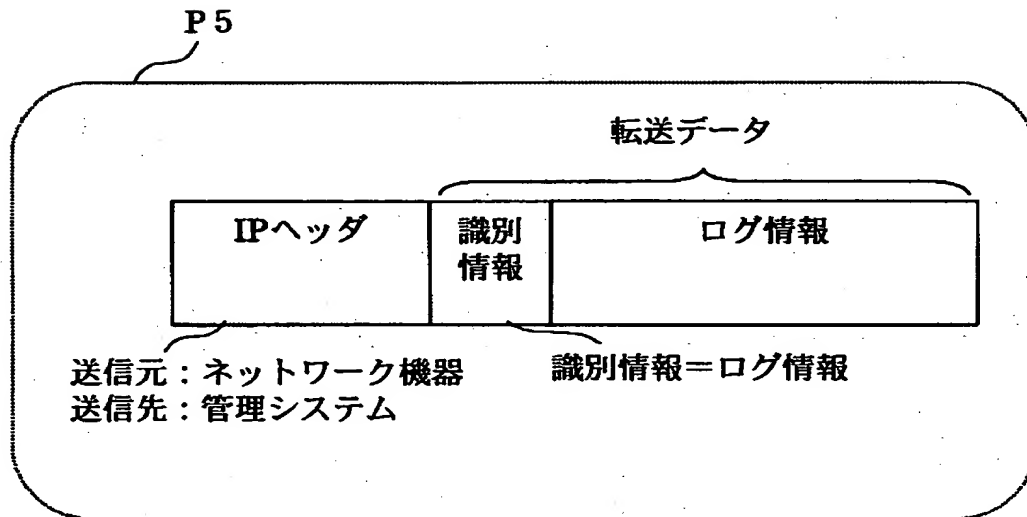
【図 7】



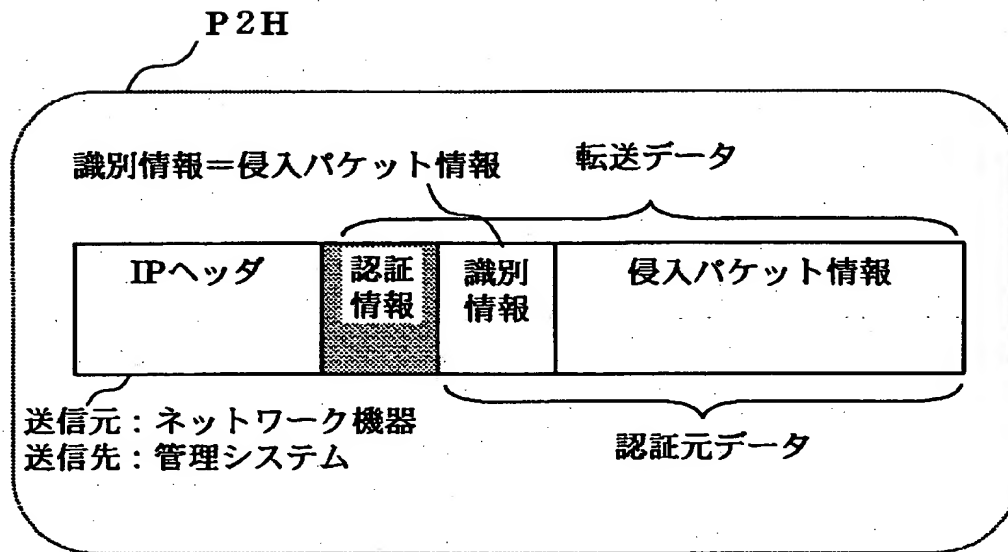
【図8】



【図9】



【図10】





【書類名】 要約書

【要約】

【課題】 不正侵入の防御や対処を行う集中管理システムを提供する。

【解決手段】 ネットワーク機器 3 は、不正侵入者端末 6 から送信された不正侵入パケット P 1 を検出し、不正侵入パケット P 1 をエンカプセル化したパケット P 2 をデータセンタ 1 に転送し、データセンタ 1 の管理システム 1 1 は、パケット P 2 を解析し、攻撃対象サーバ 5 からの応答に見せかけた、おとりサーバ 1 3 からの応答パケット P 4 をエンカプセル化してパケット P 3 とし、パケット P 3 をネットワーク機器 3 に送信し、ネットワーク機器 3 は、パケット P 3 をデカプセル化して応答パケット P 4 を取りだして不正侵入者端末 6 に送信し、これにより不正侵入者端末 6 は、応答パケット P 4 を攻撃対象サーバ 5 からの応答と思い込み、おとりサーバ 1 3 に侵入を開始する。

【選択図】 図 5

出 願 人 履 歴 情 報

識別番号 [000006013]

|          |                   |
|----------|-------------------|
| 1. 変更年月日 | 1990年 8月24日       |
| [変更理由]   | 新規登録              |
| 住 所      | 東京都千代田区丸の内2丁目2番3号 |
| 氏 名      | 三菱電機株式会社          |